IEE Proceedings of : *People in Control - An International Conference on Human Interfaces in Control Rooms, Cockpits and Command Centres*, University of Bath, UK, 21 – 23 June 1999.

SITUATIONAL AWARENESS THROUGH THE INTERFACE: EVALUATING SAFETY IN SAFETY-CRITICAL CONTROL SYSTEMS

C Sandom

ASACS Safety and Standards Unit, United Kingdom

INTRODUCTION

Modern safety-critical control systems are often highly interactive systems situated in dynamic environments. In complex systems such as these, the quality of the information acquired through the interface can contribute significantly to system failure and the design of the human-computer interface can have a profound effect on operator performance and system safety. This paper will begin with a brief discussion on the nature of safety-critical control systems and an examination of the hazards peculiar to these systems.

Metrics are present in many fields of design when there is a requirement for progressive improvement and an increasing emphasis is being placed on usability metrics for evaluating the design of interactive systems. An intuitive assumption often associated with usability is that an improvement will inevitably enhance system safety. However, it will be argued that safety and usability can be mutually exclusive properties, particularly in systems that rely on situational awareness for safe operation. If this is the case, different methods and metrics are required for evaluating safety. It is suggested that it may be more appropriate to quantify safety in terms of the level of situational awareness acquired through the interface

For many years the dominant theory underpinning cognitive models of the human user has been the model human processor proposed by Card et al (1). It is now widely recognised, however, that the information processing approach to cognition has neglected the importance of how people work when using complex systems situated in the context of the real world (2, 3). An understanding of human cognition is central to the design of interactive systems and this is particularly pertinent in safety-critical systems when the elimination of hazards is a principal concern. Situational awareness is one important phenomenon that may be useful for examining human cognition. This paper will examine the dominant theoretical perspectives on situational awareness and a synthesised, pragmatic view of this critical phenomenon is proposed.

Having suggested situational awareness as a critical attribute for interactive systems, a practical method is required to help us to evaluate this important phenomenon. This paper will conclude with a brief outline of a method of evaluating the contribution of the human-computer interface to situational awareness in a military air defence control system. The aim here is not to provide a detailed discussion of a field-study with specific findings; rather the aim is to contribute to the methodological debate surrounding the evaluation of interactive safety-critical control systems.

HAZARDS AND SAFETY-CRITICAL SYSTEMS

What is a Safety-Critical System?

Safety has only recently been placed on the agenda and recent legislation in many countries is now forcing system designers to consider safety explicitly during the development process (4). Safety engineering is a relatively new discipline and the distinction between safety-critical and safety-related systems is not clear. A comparison of the major standards in this area reveals that there is no accepted definition of the terms safety-critical and safety-related as applied to computer-based systems and the generic term *safety-significant* may be more appropriate.

While this distinction may appear to be a fatuous academic exercise, in practice, the classification of a system will often determine the stringency of the development methods adopted. For example, UK Defence Standard 00-55 requires safety-critical software components to be proven using formal methods (5). Despite this lack of clarity, the important issue is that rigorous development methods should be adopted if any system failure can initiate an ‘unintended sequence of events that causes death, injury, environmental or material damage’ (6) - irrespective of how or where that failure arises. In this area, safety attributes can be used to help designers to identify and evaluate potential system failures during the development process.

Where are the Hazards in Safety-Critical Systems?

Interactive systems present unique hazards and problems when developing safety-critical systems. Human error is repeatedly mentioned as a major contributing factor or even the direct cause of accidents or incidents. For instance, an analysis of causal factors contributing to a situation in which the safety of aircraft was compromised show that 97.7% of incidents in UK airspace during 1996 were caused by human error (calculated from (7) and (8)). Paradoxically, many system developers concentrate the majority of their efforts upon technical issues often neglecting the human contribution.

This may be due to the increased complexity introduced when dealing with the human factors of a system. While hardware reliability techniques are relatively mature and well understood, this is not the case when dealing with human reliability. It is generally very difficult to predict all the possible mental states of an operator in a complex system. Even if it were possible to identify all the possible mental states and their effects on human behaviour, the difficulty of estimating the probability of occurrence of each state remains.

Human Reliability Analysis techniques have attempted to address this issue, however, much of this research has been dominated by assumptions that apply to technical systems and often these do not translate to human systems (9). It may be argued that human error is best examined from a cognitive perspective, as traditional reliability engineering techniques do not appear to fit well with human factors concerns.

Which Hazards Are We Concerned With?

There are many different hazards associated with the operation of a typical, complex control system including those arising from both technical and human failures. The human contribution to hazards can equally arise from the inevitable errors made by operators at the ‘sharp-end’ of the system or from latent conditions introduced by system developers (10). This paper is specifically concerned with the active failures arising from knowledge-based mistakes at the ‘sharp end’ of system operation.

For complex systems in dynamic environments, an operator must to pay attention to a large volume of information from a variety of sources including sensors and other operators in order to acquire an awareness of the situation in question. Billings (11) argues that in many cases humans are no longer able to appreciate the true situation without the aid of machines, therefore, machines must tell us more of what we need to know and they must do it more effectively and less ambiguously than before.

The design of the human-computer interface (HCI) can have a profound effect on safety assurance, particularly during emergency situations. When emergencies arise and system operators must react quickly and accurately, the situational awareness of the operator is critical to their ability to make decisions, revise plans and to act purposefully to correct the abnormal situation. This sentiment emphasises the importance of designing HCIs to support situational awareness explicitly in safety-critical systems.

USABILITY AND SAFETY

The Problem with Usability Metrics

Metrics are used in many fields of design and an increasing emphasis is being placed on usability metrics for evaluating interactive systems. Usability is a fuzzy concept and there is an increasing number of ways that interface developers attempt to evaluate the usability of their products (12). Nonetheless, usability is generally taken to mean not only ease of use but the concept also equally involves effectiveness in terms of measures of human performance.

From this general definition, safety-critical system developers may be tempted to infer that a useable system is, by implication, a safe system. The intuitive assumption often underpinning the rise in importance of usability in this area is that it will inevitably lead to an improvement in safety. However, it is argued here that usability and safety can be mutually exclusive properties.

It is entirely possible that making an interactive system safe will entail many trade-offs with usability. For example, HCI prototyping may reveal a requirement for a complex keying sequence to be replaced with a macro facility allowing a function to be invoked with a single key press. This requirement may enhance system usability, however, it may inadvertently affect the safety of the system if a hazard is associated with the function being invoked. While a complex sequence may not be very efficient in terms of usability, it provides a number of opportunities for the operator to become aware that the function being invoked may be hazardous in the current context. It seems that it may not enough to simply concentrate on the usability of an interactive system to assure functionally safe operation.

Safety and Situational Awareness

The previous discussion suggests that any design trade-off between usability and safety may also affect the reliability of the cognitive processes involved with acquiring and maintaining a safe level of awareness of a situation. If a well-intentioned system designer aims to develop a transparent HCI in the name of usability, the resulting automatic interactions may have an adverse effect on the awareness of the operator. This may also affect the safety of the system. Safety must be specified in quantifiable or measurable terms in a similar manner to usability to have practical application. This may lead us to conclude that there is a case for specifying situational awareness as a suitable attribute for evaluating the safety of the HCI in safety-critical control systems.

SITUATIONAL AWARENESS – A PERSPECTIVE

What is Situational Awareness?

Situational awareness (SA) has become a common phrase for both system designers and operators who often base its use on an intuitive understanding of its definition. Sarter and Woods (13) have identified SA as a critical, but ill defined, phenomenon and others have also noted that it is difficult to find an accepted definition of the term (14). Nonetheless, SA has been the subject of much research in recent years, particularly within the field of aviation and other similarly complex domains (15, 16).

In the context of human-machine interaction, current definitions of SA are generally based on opposing views as either a cognitive phenomenon or as an observer construct; these can respectively be referred to as cognitive or interactionist perspectives. A discussion of the fundamental differences between these perspectives can be used to help to understand situational awareness in the context of safety-critical systems.

The Cognitive Perspective of SA

The cognitive perspective views SA as a phenomenon that occurs ‘in the head’ of an operator in a similar fashion to the dominant cognitive framework of the human as an information processor (1). The process-oriented view within this perspective sees SA as being acquired and maintained by the user undertaking various cognitive activities (13). Another view sees SA as a product – a state of awareness about the situation with reference to knowledge and information (17). Some researchers have even integrated these process and product perspectives (18).

Whilst these conflicting views may signify an apparent lack of coherence within the cognitive perspective, Endsley’s (19) theoretical model of SA, based on the role of SA in human decision making in dynamic systems, has been widely cited and highly influential in cognitive science research. This model represents a typical cognitive perspective and it proposes three different levels of SA which are relevant to this paper:

Level 1 SA - Perception. The perception of the status, attributes and dynamics of relevant elements in the environment.

Level 2 SA - Comprehension. The comprehension of the situation based on a synthesis of disjointed Level 1 elements to form a holistic ‘picture’ of the environment.

Level 3 SA - Projection. The projection of the near-term future of the elements in the environment.

These different levels suggest that SA is based on more than simply perceiving information about the environment, which is often the intuitive definition. Many cognitive accounts of SA suggest that after information concerning relevant elements is perceived, a representation of the situation must be formed before a decision can be made based upon current SA. This leads to another common notion that is particular to the cognitive perspective with SA often considered synonymously with mental models (19).

In this context, mental models are viewed as the subjective awareness of a situation which includes what has happened, what could happen and what a user predicts will happen based on their goals and objectives (20). Despite making an explicit link with mental models, the models of SA proposed within the cognitive perspective often do not have iterative dimensions to reflect the dynamism of SA over time. Instead they generally give models which capture or explain SA at any given instant in time.

The Interactionist Perspective of SA

The interactionist perspective typically views SA as an abstraction that exists only in the mind of an observer. From this perspective, SA is considered as a useful description of a phenomenon that can be observed in humans performing work through interacting with complex and dynamic environments (11, 21).

In contrast to cognitive definitions, Smith and Hancock (22) propose an interactionist view of SA as adaptive, externally directed consciousness, arguing that there is currently an artificial and contentious division relating to general perspectives of SA as either exclusively knowledge or exclusively process.

Smith and Hancock (22) criticise the lack of dynamism exhibited within the cognitive perspective. They contend that SA is a dynamic concept existing at the interface between a user and their environment and that SA is a generative process of knowledge creation and informed action taking as opposed to merely a snapshot of a user's mental model. This view marginalises mental models– leading to a stance on SA which may be useful given that mental models themselves are an ill-defined concept subject to much debate.

Others reflect this perspective, viewing SA as a measure of the degree of dynamic coupling between a user and a particular situation (23). From this stance, a tangible benefit of SA research is the focus on the inseparability of situations and awareness with discussions of SA focusing attention on both what is inside the head (awareness) but also what the head is inside (situation) (24).

Broadly, the interactionist view of SA is that the current awareness of a situation affects the process of acquiring and interpreting new awareness in an ongoing cycle. A key element of the interactionist view of SA is the contribution of active perception on the part of the user in making sense of the situation in which they are operating. Such active perception suggests directed consciousness on the part of the user.

A Pragmatic Perspective of SA

As the preceding discussion has highlighted, there are competing and sometimes confusing views on SA and its relation to people and the situations in which they are operating. There is currently significant on-going research to further these debates and refine these perspectives. Whilst such research is of long-term value in contributing to the maturity of the field and refining explanations of SA, this paper takes a more pragmatic approach, arguing that a view of SA that incorporates features of both the cognitive and interactionist perspectives may be more immediately useful to practitioners.

SA is a term often used intuitively to describe the experience of comprehending what is happening in a complex, dynamic environment in relation to an overall objective or goal. Regardless of theoretical perspective, it is generally accepted that this experience involves both acquiring and maintaining a state of awareness (19, 22) in a ‘continuous extraction cycle’.

The temporal nature of the continuous extraction process implies that SA requires the diagnosis of past problems and the prognosis and prevention of future problems based on an understanding of current information. Consequently, it is suggested that a pragmatic SA framework must be inherently dynamic and responsive to environmental changes.

Another concept relating to SA concerns the question of consciousness. Compare, for example, the description of Endsley’s cognitive model of SA (19) with the interactionist model prescribed by Smith and Hancock (22) in the previous discussion. It is suggested that the passive, information-processing model of cognition (upon which a cognitive perspective of SA is often founded) is invalid. This does not mean to imply that the cognitive perspective is worthless; clearly this paradigm has contributed substantially to research. However, it is argued that this perspective has become a constraining factor and a different paradigm is required to accommodate the existence of deliberate action in SA research. Thus, in a similar manner to the interactionist proponents of SA, it is suggested that an individual’s awareness of an objective situation consciously effects the process of acquiring and interpreting new awareness in an continuous, proactive extraction cycle.

This pragmatic perspective acknowledges the equal importance of both the product of SA and the dynamic process of directed consciousness required to acquire and maintain SA. Within this perspective, SA can broadly be viewed as the fit between a subjective interpretation (awareness) of a situation, built through the individual's interaction with their environment, and an objective measure of the situation (26). Such a view of SA suggests that a strong correspondence between the subjective interpretation and the objective situation indicates high SA while weak correspondence means low SA. It is important to recognise that SA is viewed here as an abstraction that exists only *in the mind of the observer* describing phenomena that can be observed in humans performing work (interacting) in complex, dynamic environments.

So far we have only considered the theoretical principles of SA. Practical methods are required to help us to evaluate the design of interactive systems and specifically to measure their contribution to SA. A summary of a field-study of a military air defence control system is presented here to illustrate one method of measuring the safety of an interactive system.

EVALUATING SAFETY IN INTERACTIVE SYSTEMS

System Description

The United Kingdom Air Defence Ground Environment (UKADGE) system provides ground-based command and control services to military aircraft within the UK. The core capability of the UKADGE system is provided by the Air Traffic Control activity of Air Defence Fighter Controllers and also by the hardware and software of a system known as the Integrated Command and Control System (ICCS) which, together with data from other sources can compile an air picture of the UK.

The existing ICCS hardware is becoming obsolete and expensive to maintain and a project is being undertaken to replace the system with more modern, commercial off-the-shelf components. Many of the system changes will be transparent to the Fighter Controllers; however, a major tangible change will occur with the replacement of the existing ICCS HCI which will impact significantly on system interactions and activities.

From an operational safety perspective, the proposed changes to the system HCI have been recognised as a major area of risk and a pragmatic method of assessing the relative functional safety of the replacement system was required. An empirical study of the UKADGE system was therefore undertaken to provide a method of assessing the relative safety of the existing HCI and to collect benchmark data against which a replacement HCI could be evaluated.

A preliminary survey was conducted at all UK Air Defence sites using semi-structured interviews with a representative sample of Fighter Controllers and a questionnaire was distributed to all Fighter Controllers to identify representative air traffic control activities (Air Defence missions) for analysis. Significantly, this preliminary survey revealed that all Fighter Controllers regarded SA as a major safety concern for operators of this safety-critical system. Consequently, a method of evaluating the contribution of the HCI design to SA was required.

Safety Evaluation Method

A Safety Study of the UKADGE system was undertaken based on the pragmatic perspective of SA outlined previously. The study was planned to be conducted in three distinct phases:

Scenario Development Phase. Data was obtained from an operational Air Defence site based on live operations. Specifically, video and voice recordings were obtained from a number of Fighter Controllers during live operational sorties as identified during the preliminary survey. Post-task analyses were conducted with the Fighter Controllers to identify critical interaction points and to elicit suitable SA probe questions which were to be used during the Simulation Phase. Plot and track data recordings were also collected to assist with the development of high-fidelity simulations.

Simulation Phase. The plot and data recordings collected during the Scenario Development phase were used to generate realistic control scenarios based on the observed live operations. Simulations were then run in an operational environment using a number of Fighter Controllers for each different scenario. This phase provided additional qualitative data and much finer quantitative evaluation data relating to the HCI design and the product and processes of SA.

Safety Evaluation Phase. This phase would be the responsibility of the implementation contractor who would be required to demonstrate the relative safety of the replacement HCI based exactly on the scenarios and metrics derived during the Scenario Development and Simulation Phases.

Collecting Safety Metrics

Having decided upon a method for conducting the safety study, it was also necessary to specify exactly how the benchmark SA data would be collected during the Simulation Phase. From the previous discussion, it was determined that a pragmatic approach would require both the *product* and the *process* of SA to be assessed to provide meaningful benchmark metrics and data for evaluating the relative safety of existing and replacement HCIs.

Evaluating the Product of SA. Endsley's (26) Situation Awareness Global Assessment Technique (SAGAT) was used to evaluate the level of the operator's subjective awareness during the field-study. Briefly, the SAGAT technique requires the simulation to be frozen at different points and the operator answers domain-specific probe questions to quantify their awareness of the situation. The quantitative results from each simulation is taken as the safety benchmark for the HCI in terms of its SA support.

Evaluating the Process of SA. Sandom and Macredie's (27) Dynamic Model of SA was used as a framework for identifying problems associated with the *process* of acquiring and maintaining SA in this safety-critical environment. The model was specifically used to identify potential or actual interaction problems relating to SA and safety. This data was used to produce a qualitative evaluation of how the HCI design supports the process of acquiring and maintaining operator awareness.

SUMMARY

This paper has made a case for Situational Awareness (SA) as a critical attribute for evaluating the safety of HCIs in safety-critical control systems by quantifying the level of SA acquired through the interface. It was suggested that SA is a dynamic concept that exists at the interface between an operator and the environment. A pragmatic definition of SA was given as the fit between a subjective interpretation (awareness) of a situation and an objective measure of the situation built through an individual's interaction with their environment.

Based on this perspective, it was suggested that SA can provide safety-critical interactive systems designers with a quantitative measure of the dynamic coupling between an operator and a particular situation. From this discussion, it is a contention of this paper that SA is a critical safety attribute that can be used in the context of interactive systems to quantify the relative safety of a human-computer interface.

The paper has presented aspects of a field-study of a military air defence system and indicated a method of evaluating the process and the product of SA to produce benchmark data relating to the safety of a system interface. The initial findings of the field-study have already directed the developers to specify SA as a critical safety attribute for the replacement interface. The safety requirements for the replacement system now specify that the replacement system must balance the requirements of both SA and usability in the design of interfaces and interactions.

This study is on-going and initial experiences suggest that an SA-based approach to system evaluation and design has the potential for further contribution to the design of the military control system HCI and to safety-critical control systems in general.

ACKNOWLEDGEMENTS

I am indebted to Robert Macredie from Brunel University for contributing to the development of the ideas presented in this paper. I would also like to thank my ASSU colleagues who reviewed this paper.

REFERENCES

1. Card S. K., Moran T. P. and Newell A., 1983, “The Psychology of Human Computer Interaction”, Lawrence Erlbaum Associates, Hillsdale, New Jersey.

2. Suchman L., 1987, “Plans and Situated Actions”, Cambridge, Cambridge University Press.

3. Winograd T. and Flores F., 1986, “Understanding Computers and Cognition: A New Foundation for Design”, Norwood, Ablex.

4. IEE, 1995, “Safety-Related Systems: Guidance for Engineers”, IEE Hazards Forum, March.

5. MoD, 1996, “Requirements for Safety Related Software in Defence Equipment”, Defence Standard 00-55, July.

6. MoD, 1996, “Safety Management Requirements for Defence Systems”, Defence Standard 00-56(Part1)/Issue2, December 1996.

7. CAA, 1998, “Aircraft Proximity Reports: Airprox (C) - Controller Reported”, August 1997 - December 1997, Vol 13, Civil Aviation Authority, London, March.

8. CAA, 1998, “Analysis of Airprox (P) in the UK: Join Airprox Working Group Report No. 3/97”, September 1997 - December 1997, Civil Aviation Authority, London, August.

9. Woods D.D., Johannesen L. J., Cook R. I. and Sarter N. B., 1994, “Behind Human Error: Cognitive Systems, Computers and Hindsight”, CSERIAC 94-01.

10. Reason J., 1997, “Managing the Risks of Organizational Accidents”, Ashgate.

11. Billings C. E., 1995, Situation Awareness Measurement and Analysis: A Commentary, in (16).

12. Smith A., 1997, “Human-Computer Factors: A Study of Users and Information Systems”, London, McGraw Hill.

13. Sarter N. B. and Woods D. D., 1991, “Situation Awareness: A Critical but Ill-Defined Phenomenon”, Int J of Aviation Psychology, 1, 45-57.

14. Hopkin V. D., 1995, “Human Factors in Air Traffic Control”, Taylor and Francis.

15. Harris D., Ed., 1997, “Engineering Psychology and Cognitive Ergonomics Volume 1: Transportation Systems”, Proc. 1st Int. Conf EP&CE, Ashgate Publishing.

16. Garland D. J. and Endsley M. R., Eds., 1995, “Experimental Analysis and Measurement of Situation Awareness”, Proc. of an Int Conf, FL:USA, November.

17. Endsley M. R., 1995, Theoretical Underpinnings of Situation Awareness: A Critical Review, in (16).

18. Isaac A. R., 1997, Situational Awareness in Air Traffic Control: Human Cognition and Advanced Technology, in (15).

19. Endsley M. R.,1995, “Towards a Theory of Situation Awareness in Dynamic Systems”, Human Factors, 37, (1), 32-64, March.

20. Kirwan B., Donohoe L., Atkinson T., MacKendrick H., Lamoureux T. and Phillips A., 1998, “Getting the Picture: Investigating the Mental Picture of the Air Traffic Controller”, Proc. Conf. Ergonomics Society, 405-408.

21. Flach J. M., 1995, “Situation Awareness: Proceed with Caution”, Human Factors, 37, (1), 149-157, March.

22. Smith K. and Hancock P. A., 1995, “Situation Awareness is Adaptive, Externally Directed Consciousness”, Human Factors, 37, (1), 137-148, March.

23. Flach J. M., 1995, Maintaining Situation Awareness when Stalking Cognition in the Wild, in (16).

24. Mace W. M., 1977, Ask Not What’s Inside Your Head But What Your Head’s Inside Of, in Shaw R. E. and Brandsford J., Eds., “Perceiving, Acting and Knowing”, Hillsdale NJ, Erlbaum.

25. Flach J. M., 1996, “Situation Awareness: In Search of Meaning”, CSERIAC Gateway, 6, (6), 1-4, 1996.

26. Endsley M. R., 1995, “Measurement of Situation Awareness in Dynamic Systems”, Human Factors, 37, (1), 65-84, March.

27. Sandom C. and Macredie R. D., 1998. “Do You Get The Picture? Situation Awareness and Safety-Critical Interactive Systems” submitted to ACM ToCHI, Special Issue: Interface Issues and Designs for Safety-Critical Interactive Systems, December.